FortiClient™ Connect Endpoint Security System

Release Notes

FortiClient Connect for Mac

v4.0

04-400-144164-20110630

FORTINET

Table of Contents

1 FortiClient Connect for Mac v4.0 1
1.1 What's New 1
1.2 Documentation 1
1.3 Language Support 1
1.4 Licensing 2
1.5 Supported Operating System 2
1.6 System Requirements 2
2 Special Notices 3
2.1 General 3
2.2 Reconnect after resuming from Mac Sleep/Hibernate/Standby 3
3 Upgrade and Installation Information 4
4 Known Issues in FortiClient Connect for Mac v4.0 5
5 Appendix 6
5.1 How to Configure IPSec VPN 6
5.1.1 IPSec VPN Configuration Instruction for FortiOS v4.0 MR3 6
5.1.2 IPSec VPN Configuration Instruction for FortiClient Connect v4.0 MR3 6
5.1.3 IPSec VPN Configuration Instruction for FortiOS v4.0 MR2 6

Change Log

Date	Change Description
2011-06-30	Initial Release

© Copyright 2011 Fortinet Inc. All rights reserved.
Release Notes FortiClient™ Connect for Mac v4.0.

Trademarks
Copyright© 2011 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions. Network variables, different network environments and other conditions may affect performance results, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding contract with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.

Support will be provided to customers who have purchased a valid support contract. All registered customers with valid support contracts may enter their support tickets via the support site: https://support.fortinet.com

1 FortiClient Connect for Mac v4.0

This document provides a summary of the new features in FortiClient Connect for Mac v4.0 and provides information on installation instructions and known issues. The FortiClient Connect for Mac v4.0 is also known as v4.0.0.113.

1.1 What's New

The following is a brief list of the new features added in FortiClient Connect for Mac v4.0.

- Introduces New web UI design
- Simplified SSLVPN Feature
- Enhanced IPSec VPN Feature
- Supports Mac Keychain for Certificate
- Introduces VPN HomePage View Option

1.2 Documentation

The following documentation is available from the Fortinet Technical documentation website at http://docs.fortinet.com

- FortiClient Connect for Mac Quickstart Guide
- FortiClient Connect for Mac Deployment Guide

Articles and information on specific issues are available from the Fortinet Knowledge Base at http://kb.fortinet.com

1.3 Language Support

FortiClient Connect for Mac v4.0 is localized for the following languages:

	GUI	Documentation
English	Yes	Yes
French	-	-
German	-	-
Japanese	-	-
Portuguese (Brazilian)	-	-
Spanish (Spain)	-	-
Slovak	-	-
Czech	-	-

1.4 Licensing

Licensing of FortiClient Connect for Mac is controlled by FortiOS v4.3. The user has to buy the FortiClient Connect license with FortiGate Support Contract, based on the number of simultaneous active VPN connections to the FortiGate.

1.5 Supported Operating System

The following operating systems are supported:

- Mac OS X Leopard (v10.5)
- Mac OS X Snow Leopard(v10.6)

1.6 System Requirements

FortiClient Connect for Mac v4.0 has the following minimum system requirements:

- Intel Processor
- 256MB of RAM
- 20MB of disk space
- TCP/IP communication protocol
- Ethernet NIC for network connections
- Wireless adapter for wireless network connections
- Adobe Acrobat Reader for user Manual

2 Special Notices

2.1 General

FortiClient Connect for Mac v4.0 supports import of unencrypted VPN configuration file created using FortiClient Connect for Windows 4.3.

2.2 Reconnect after resuming from Mac Sleep/Hibernate/Standby

Any active VPN connection will be disconnected when Mac enters Sleep/Hibernate/Standby mode, user will have to reconnect after Mac resumes.

3 Upgrade and Installation Information

This is a first release of the FortiClient Connect for Mac software, so upgrades from previous versions do not apply.

Note: Uninstall any previous beta version of FortiClient Connect for Mac (also remove the Fortinet folder in 'Library/Application Support' directory) before installing FortiClient Connect for Mac v4.0.

4 Known Issues in FortiClient Connect for Mac v4.0

This section lists the known issues of this release, but is NOT a complete list.

Description: The setting change for a new log level will not apply until FortiClient Connect restarts

Bug ID: 148113
Status: N/A

Workaround: Restart FortiClient Connect.

Description: A warning message about “FCTUgrader” may pop up after install.

Bug ID: 147729
Status: N/A
Workaround: Acknowledge the warning message.

Description: SSL VPN does not give warning message when Remote Gateway locks the connection after several bad login attempts.

Bug ID: 146002
Status: N/A
Workaround: Reconnect with correct login credentials after the lock is expired.

Description: Error message sometimes does not contain meaningful feedback.

Bug ID: 144252
Status: N/A
Workaround: NA

Description: When save a failed connection using Quick Connect, null connections are created and displayed in the VPN connection list

Bug ID: 147971
Status: N/A
Workaround: The Null connections are automatically removed after FortiClient Connect restarts.

5 Appendix

5.1 How to Configure IPSec VPN

5.1.1 IPSec VPN Configuration Instruction for FortiOS v4.0 MR3

Described below are the steps to configure an interface mode IPSec VPN on FortiOS v4.0 MR3.

Step 1: On the FortiGate (running v4.0 MR3) go to VPN > IPSec > Auto Key (IKE) page.
Step 2: Click on “Create FortiClient VPN” button.
Step 3: Fill the VPN tunnel configuration details on the page and click OK.
Step 4: Verify that a Phase1 and Phase2 has been created for the VPN.
Step 5: Configure appropriate firewall policies under Firewall > Policy page for VPN traffic.

5.1.2 IPSec VPN Configuration Instruction for FortiClient Connect v4.0 MR3

Described below are the steps to configure an interface mode IPSec VPN on FortiClient Connect v4.0 MR3.

Step 1: Open the FortiClient console and navigate to IPSec VPN main page.
Step 2: Click '+' icon on the bottom-left corner to add a new connection.
Step 3: Input the following information on the "Add Connection" page.

- Connection Name
- Remote Gateway
- Authentication Method
- XAuth
- Click OK

Step 4: Select the VPN connection from the list and click *Connect* to establish the IPSec tunnel.

5.1.3 IPSec VPN Configuration Instruction for FortiOS v4.0 MR2

Described below are the steps to configure an interface mode IPSec VPN on FortiOS v4.0 MR2.

Step 1: Create an address name for internal subnet if it doesn’t exist yet. (Optional)
Step 2: Create an user group for FortiClient users on User > User Group web UI page.
Step 3: Navigate to VPN > IPsec > Auto Key > Create Phase1 web UI page and input the following information:

- Name (i.e. mydialup-phase1)
- Remote Gateway (i.e. Dialup User)
- Local Interface (i.e wan1)
- Mode: *Aggressive*
- Authentication Method
- Enable *IPSec Interface Mode* option
- XAUTH: *Enable as server*

- User Group: <*select the FortiClient user group*>
- Click OK

Step 4: Navigate to VPN > IPsec > Auto Key > Create Phase2 web UI page and input the following information:

- Name (i.e. mydialup-phase2)
- Phase1: *select the phase1 VPN created before* (i.e. mydialup-phase1)
- Click OK

Step 5: From the FortiGate CLI, enter the following commands:

- config vpn ipsec phase1-interface
  edit <phase1 name>
  set mode-cfg enable
  set ipv4-start-ip <start ip address>
  set ipv4-end-ip <end ip address>
  set ipv4-netmask <network mask>
  set ipv4-split-include <address group> (optional setting)
  set ipv4-dns-server1 <server ip> (optional setting)
  end
- Click OK

Step 6: Configure appropriate firewall policies using Firewall > Policy page for VPN traffic.

(End of Release Notes.)